IN THE CLAIMS

1. (original) In a data processing system, a method comprising the steps of:

creating a migratable storage tree with a storage root key; and

creating a non-migratable storage tree with the storage root key, wherein the migratable storage tree and the non-migratable storage tree are identically structured.

a1

2. (original) The method as recited in claim 1, wherein the migratable storage tree and the non-migratable storage tree are created by a trusted computing module in accordance with Trusted Computing Platform Alliance.

3. (original) The method as recited in claim 1, wherein the migratable storage tree comprises migratable keys and a user key, wherein the non-migratable storage tree comprises non-migratable keys and a user key.

4. (original) The method as recited in claim 1, wherein the non-migratable storage tree will include non-migratable storage keys corresponding to each migratable storage key in the migratable storage tree.

5. (original) The method as recited in claim 1, wherein use authorization in the non-migratable storage tree will be identical to use authorization in the migratable storage tree.

6. (original) The method as recited in claim 1, further comprising the steps of:

requesting a migratable storage key; and

requesting a non-migratable storage key.

7. (original) The method as recited in claim 6, wherein the step of requesting a migratable storage key will identify a parent key in the migratable storage tree, and wherein the step of

requesting a non-migratable storage key will identify a parent key in the non-migratable storage tree that corresponds to the parent key in the migratable storage tree.

8. (original) The method as recited in claim 1, further comprising the step of:

when a key loading request is made for a migratable storage key, loading a key from the non-migratable storage tree instead of loading a corresponding key from the migratable storage tree.

9. (original) In a data processing system, a method comprising the steps of:

splitting a request to create a new migratable storage key with given authentication data and a first parent key into first and second commands;

wherein the first command creates a migratable storage key with the given authentication data and the first parent key; and

wherein the second command requests creating a non-migratable storage key with the given authentication data and a second parent key which is determined from looking up a key that corresponds to the first parent key in a database.

10. (original) The method recited in claim 9, wherein the migratable storage key and the non-migratable storage key are associated in a database.

11. (original) The method recited in claim 9, wherein the non-migratable key is a multi-prime key.

12. (original) The method recited in claim 9, where the non-migratable key is an elliptic curve key.

13. (original) The method as recited in claim 9, further comprising the steps of:

creating a new migratable signing key with the given authentication data and a third parent key;

a1

storing the new migratable signing key with the given authentication data and the third parent key;

storing the new migratable signing key with the given authentication data and a fourth parent key where the fourth parent key is a non-migratable key associated with the third parent key in a database.

14. (original) The method as recited in claim 13, further comprising the steps of:

requesting a signature by the new migratable signing key;

searching the database for the location of a key blob containing the new migratable signing key;

loading a copy of the new migratable signing key stored in the key blob created with the non-migratable parent key; and

signing with the new migratable signing key.

15. (original) The method as recited in claim 9, further comprising the steps of:

creating a new data stored by means of the first parent key;

storing the new data with the first parent key;

storing the new data with the second parent key where the second parent key is a non-migratable key associated with the third parent key in a database.

16. (original) The method as recited in claim 15, further comprising the steps of:

requesting data stored by the new migratable storage key;

searching the database for the location of a key blob associated with the new migratable storage key;

loading a copy of the key blob created with the non-migratable storage key; and decrypting the data.

17. (original) The method as recited in claim 14, further comprising the steps of:

requesting migration of new migratable signing keys;

searching the database for the location of a key blob associated with a non-migratable parent of the key to be migrated;

processing the migration.

18. (original) In a data processing system, a method comprising the steps of:

creating a migratable storage tree with a storage root key; and

creating a non-migratable storage tree with the storage rootkey where the migratable storage tree and the non-migratable storage tree are identically structured with corresponding keys and authentication data.

19. (original) The method as recited in claim 18, wherein the migratable storage tree and the non-migratable storage tree are created by a trusted computing module in accordance with Trusted Computing Platform Alliance.

20. (original) The method as recited in claim 19, wherein the migratable storage tree comprises migratable keys and a user key, wherein the non-migratable storage tree comprises non-migratable keys and a user key.

21. (original) The method recited in claim 18, wherein the migratable storage tree comprises migratable keys and encrypted user data wherein the non-migratable storage tree comprises non-migratable keys and encrypted user data .

22. (original) The method as recited in claim 18, wherein the non-migratable storage tree will include non-migratable storage keys corresponding to each migratable storage key in the migratable storage tree.

23. (original) The method as recited in claim 18, wherein the non-migratable storage tree will include non-migratable storage keys corresponding to a subset of the migratable storage keys in the migratable storage tree.

24. (original) The method as recited in claim 18, wherein use authorization in the non-migratable storage tree will be identical to use authorization in the migratable storage tree.

25. (original) The method as recited in claim 18, wherein use authorization in the non-migratable storage tree can be deduced from user authorization in the migratable storage tree with additional data.

26. (original) The method as recited in claim 25, wherein the use authorization in the non-migratable storage tree is obtained by hashing the concatenation of the user authorization in the migratable storage tree with a fixed string.

27. (new) The method as recited in claim 1, wherein a migratable key can be transferred to other trusted platform module chips, and wherein a non-migratable key cannot be transferred to other trusted platform module chips.